Claim Amendments

1. (canceled)

2. (amended) A digital optical medium containing compressed digital audiovisual content with protections against unauthorized copying, comprising:

(a) a digital signature authenticating at least an identifier of said optical medium;

(b) a ~~digitally signed~~ revocations list identifying at least one other medium that is revoked;

(c) compressed digital audiovisual content that is encrypted using broadcast encryption, whereby:

(i) each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting said audiovisual content, and

(ii) each of a plurality of revoked playback devices do not have keys sufficient for decrypting said audiovisual content;

(d) program logic for an interpreter of a Turing complete language, the program logic adapted for execution on a playback device in order to play said audiovisual content, the program logic installing on the playback device and cryptographically protecting on the playback device the revocations list;

[[~~(d)~~]](e) a plurality of versions for each of a plurality of portions of said compressed digital audiovisual content, where:

(i) said versions for each portion may be distinguished from each other in pirated recordings of said audiovisual content;

(ii) said versions are encrypted with different keys, such that each of said authorized playback devices is capable of deciphering at least one, but not all, of said versions for each of said portions; and

(iii) the combination of said portions decipherable by a given player may be used to identify said player; and

[[~~(e)~~]](f) logic defining an interface usable to interact with a user and to control playback of said audiovisual content.

3. (amended) The medium of claim 22 where: ~~further comprising program logic for an interpreter of a Turing-complete language, where:~~

(i) said program logic is configured to perform a plurality of said security checks; and

(ii) said program logic is configured to permit playback of said audiovisual content provided that said plurality of security checks are successful.

4. (original) The medium of claim 3 where said program logic is configured to invoke at least one cryptographic operation supported by at least one of said authorized playback devices.

5. (original) The medium of claim 3 where said program logic is configured to perform at least one operation necessary for decryption of said audiovisual content by at least one said authorized playback device.

6. (original) The medium of claim 2 wherein a subset of said authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and further comprising program logic which, when executed by a device of each said vulnerable model, is configured to:

(a) mitigate said vulnerability affecting said vulnerable playback device; and

(b) perform at least one operation necessary for said vulnerable playback device to decrypt said audiovisual content.

7. (original) The medium of claim 6 where said program logic includes executable code for a Turing-complete virtual machine.

8. (original) The medium of claim 6 where said operation necessary to decrypt includes updating a cryptographic key contained in said playback device.

9. (original) The medium of claim 6 where said program logic for mitigating includes native executable code configured to detect whether the security of a vulnerable device has been compromised.

10. (original) The medium of claim 6 where said program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device.

11. (original) The medium of claim 6 where said program logic for mitigating includes a firmware upgrade for correcting at least one vulnerability.

12. (amended) A device for securely playing digital audiovisual content, said audiovisual content including a plurality of regions each having multiple versions thereof, comprising:

(a) a media drive including a laser for use in reading data from rotating optical media;

(b) a nonvolatile memory containing:

(i) a set of cryptographic player keys for use with a broadcast encryption system, and

(ii) identifiers of revoked media;

(c) a bulk decryption module for decrypting encrypted audiovisual content from said media;

(d) a Turing-complete interpreter for executing program logic configured to:

(i) install from the media drive and cryptographically protect in the nonvolatile memory identifiers of revoked media;

(ii) verify whether valid digital signatures contained on said media authenticate said media; and

(iii) verify whether said media are identified as revoked in said nonvolatile memory;

(iv) select a version of each said region;

([~~ii~~]v) decrypt said selected version(s), whereby a combination of said versions selected in the course of playing said media uniquely identifies said device; and

(e) at least one codec for decompressing said audiovisual content~~; and~~

~~(f) media verification logic configured to verify:~~

~~(i) whether valid digital signatures contained on said media authenticate said media, and~~

~~(ii) whether said media are identified as revoked in said nonvolatile memory~~.

13. (original) The device of claim 12 further comprising an interpreter for a Turing-complete language, where said interpreter is configured to obtain said program logic from said drive and execute said program logic.

14. (amended) The device of claim 12 further comprising means for reducing during a rendering process the output quality of said audiovisual content [[~~if~~]] in dependence upon whether a security requirement specified by said medium for high-quality output is [[~~not~~]] met.

15. (previously presented) The device of claim 12 wherein:

(a) said combination of versions selected during the course of playback of any one said medium does not uniquely identify said playback device; and

(b) said combination of versions selected during the course of playback of a plurality of said media does uniquely identify said playback device.

16. (amended) A method for playing encrypted digital audiovisual content from a digital medium, comprising:

(a) verifying a digital signature authenticating said medium;

(b) retrieving at least one player key from a nonvolatile memory;

(c) using said at least one player key with a broadcast encryption system;

(d) using a result of said broadcast encryption system to decrypt at least a portion of said audiovisual content;

(e) reading program logic for a Turing-complete interpreted language from the digital medium;

(f) using an interpreter to execute said program logic, where said interpreter performs operations specified in said program logic [[~~to respond to selections from a user~~]] including

(i) installing from the media drive and cryptographically protecting identifiers of revoked media;

(ii) verifying whether valid digital signatures contained on said media authenticate said media; and

(iii) verifying whether said media are identified as revoked in said nonvolatile memory;

(g) selecting a variant from a plurality of variants for each of a plurality of portions of said audiovisual content, where:

(i) said player is capable of decrypting said selected variant; and

(ii) said player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each said portion; and

(h) decrypting each said selected variant.

17. (amended) The method of claim 16 where said interpreter performs operations specified in said program logic to respond to selections from a user, said user selections include button presses on a remote control.

18. (original) The method of claim 16 where said program logic directs said player to perform an AES block cipher operation via said interpreter.

19. (previously presented) The method of claim 16 further comprising accessing a media revocations list to determine whether said medium has been revoked.

20. (twice amended) The device of claim 12 [[~~,~~]] where:

said set of cryptographic player keys is unique to the player; and

said program logic is configured to select a unique set of versions representing the content using said unique set of cryptographic player keys.

21. (New) The medium of claim 3 where results of the program logic is adapted to embed the results of the at least one security check into audio visual content rendered by the playback device on which security checking is performed.

22. (New) The medium of claim 2 where the program logic is adapted to perform at least one security check of a playback device seeking to play said audiovisual content, the at least one security check adapted to verify at least one of (i) playback device identity, including at least one of player serial number, specific subscriber information, player model, or player software version, or (ii) a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device.

23. (New) The device of claim 12 where the media verification logic further performs a security check that interrogates playback environment to verify at least one of (i) playback device identity, including at least one of player serial number, specific subscriber information, player model, or player software version, or (ii) a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device.

24. (New) The device of claim 12 where the Turing-complete interpreter is adapted to execute program logic that does not decrypt a selected version if the program logic identifies said media as revoked.

25. (New) The method of claim 16 where said program logic performs at least one security check of a player device seeking to play said audiovisual content, the at least one security check adapted to verify at least one of (i) player identity, including at least one of player serial number, specific subscriber information, player model, or player software version, or (ii) a result of cryptographic processing adapted to fail verification operation if executed on at least one of an

unauthorized or revoked or compromised player, and to inhibit at least one of full quality playback or playback if at least one security check fails.